Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/GB05/001709

International filing date: 04 May 2005 (04.05.2005)

Document type: Certified copy of priority document

Document details: Country/Office: GB
Number: 0410975.7
Filing date: 17 May 2004 (17.05.2004)

Date of receipt at the International Bureau: 06 June 2005 (06.06.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)

PCT/GB2005/001709.

INVESTOR IN PEOPLE

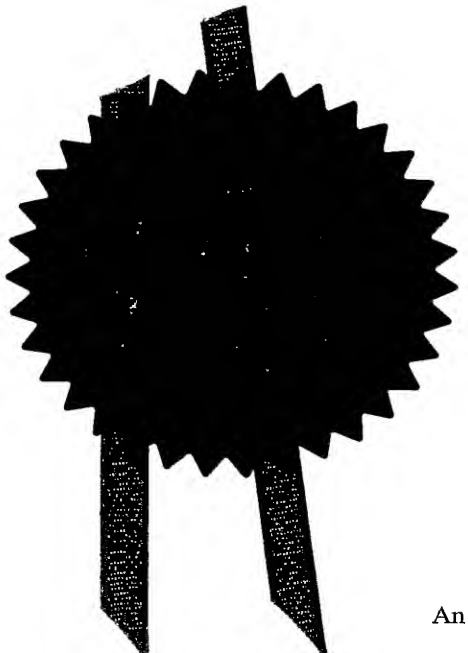
The Patent Office
Concept House
Cardiff Road
Newport
South Wales
NP10 8QQ

I, the undersigned, being an officer duly authorised in accordance with Section 74(1) and (4) of the Deregulation & Contracting Out Act 1994, to sign and issue certificates on behalf of the Comptroller-General, hereby certify that annexed hereto is a true copy of the documents as originally filed in connection with the patent application identified therein.

In accordance with the Patents (Companies Re-registration) Rules 1982, if a company named in this certificate and any accompanying documents has re-registered under the Companies Act 1980 with the same name as that with which it was registered immediately before re-registration save for the substitution as, or inclusion as, the last part of the name of the words "public limited company" or their equivalents in Welsh, references to the name of the company in this certificate and any accompanying documents shall be treated as references to the name with which it is so re-registered.

In accordance with the rules, the words "public limited company" may be replaced by p.l.c., plc, P.L.C. or PLC.

Re-registration under the Companies Act does not constitute a new legal entity but merely subjects the company to certain additional company law rules.

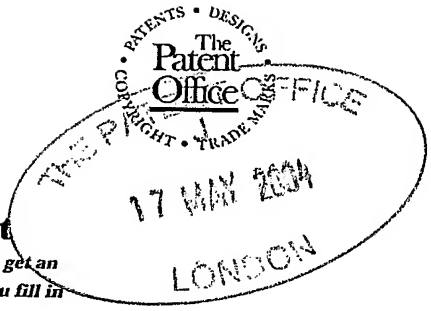


Signed K Behen

Dated 25 May 2005

Patents Form 1/77

Patents Act 1977
(6)



1/77

Request for grant of a patent

(See the notes on the back of this form. You can also get an explanatory leaflet from the Patent Office to help you fill in this form)

The Patent Office

Cardiff Road
Newport
South Wales
NP10 8QQ

1. Your reference

DRW/P17153

2. Patent application number
(The Patent Office will fill in this part)

0410975.7

18MAY04 E896642-3 D10121
P01/7700 0.00-0410975.7 ACCOUNT CHA

17 MAY 2004

3. Full name, address and postcode of the or of each applicant *(underline all surnames)*

NDS LIMITED,
One London Road,
Staines, Middlesex TW18 4EX

Patents ADP number *(if you know it)* 7296197007

If the applicant is a corporate body, give the country/state of its incorporation

4. Title of the invention

CHIP SHIELDING SYSTEM AND METHOD

5. Name of your agent *(if you have one)*

MARKS & CLERK,

"Address for service" in the United Kingdom to which all correspondence should be sent *(including the postcode)*

Clifford's Inn Fetter Lane,
London, EC4A 1BZ

Patents ADP number *(if you know it)* 8840936001 ~~240001~~

6. If you are declaring priority from one or more earlier patent applications, give the country and the date of filing of the or of each of these earlier applications and *(if you know it)* the or each application number

Country	Priority application number *(if you know it)*	Date of filing *(day / month / year)*

7. If this application is divided or otherwise derived from an earlier UK application, give the number and the filing date of the earlier application

Number of earlier application	Date of filing *(day / month / year)*

8. Is a statement of inventorship and of right to grant of a patent required in support of this request? *(Answer 'Yes' if:*

a) any applicant named in part 3 is not an inventor, or
b) there is an inventor who is not named as an applicant, or
c) any named applicant is a corporate body.
See note (d))

YES

Patents Form 1/77

9. Enter the number of sheets for any of the following items you are filing with this form. Do not count copies of the same document

Continuation sheets of this form	
Description	7
Claim *(s)*	1
Abstract	
Drawing *(s)*	2

10. If you are also filing any of the following, state how many against each item.

Priority documents	
Translations of priority documents	
Statement of inventorship and right to grant of a patent *(Patents Form 7/77)*	
Request for preliminary examination and search *(Patents Form 9/77)*	
Request for substantive examination *(Patents Form 10/77)*	
Any other documents *(please specify)*	

11. I/We request the grant of a patent on the basis of this application.

Signature: D. White

Date: 17th May 2004

12. Name and daytime telephone number of person to contact in the United Kingdom: Duncan White 02074054916

Warning

After an application for a patent has been filed, the Comptroller of the Patent Office will consider whether publication or communication of the invention should be prohibited or restricted under Section 22 of the Patents Act 1977. You will be informed if it is necessary to prohibit or restrict your invention in this way. Furthermore, if you live in the United Kingdom, Section 23 of the Patents Act 1977 stops you from applying for a patent abroad without first getting written permission from the Patent Office unless an application has been filed at least 6 weeks beforehand in the United Kingdom for a patent for the same invention and either no direction prohibiting publication or communication has been given, or any such direction has been revoked.

Notes

a) *If you need help to fill in this form or you have any questions, please contact the Patent Office on 08459 500505.*

b) *Write your answers in capital letters using black ink or you may type them.*

c) *If there is not enough space for all the relevant details on any part of this form, please continue on a separate sheet of paper and write "see continuation sheet" in the relevant part(s). Any continuation sheet should be attached to this form.*

d) *If you have answered 'Yes' Patents Form 7/77 will need to be filed.*

e) *Once you have filled in the form you must remember to sign and date it.*

f) *For details of the fee and ways to pay please contact the Patent Office.*

CHIP SHIELDING SYSTEM AND METHOD

FIELD OF THE INVENTION

The present invention relates to protecting integrated circuit chips from invasive attack through the use of a shield.

BACKGROUND OF THE INVENTION

Security chips are of use to those wanting to protect information, data transmissions or value (typically monetary). These security chips protect data by storing it in secure memory or transmit data securely through the use of cryptography implemented on chip. There are many reasons for using these products including secure banking cards, secure access systems and secure personal identity systems. It is known in the art to protect these chips from invasive attacks whereby criminals and other agents attack the card to try to obtain, change or use secret information on the card.

One type of attack involves trying to place contacts onto internal chip nodes in order to read internal data traffic. This may be achieved by probing, using fine needles to break through the surface passivation to reach the fine metal tracks. Alternatively focused ion beam (FIB) may be used to deposit pads of metal onto the tracks for subsequent probing or bonding by wires. However it is achieved, measuring the signals on internal chip nodes represents an attack, and if successful this attack may render the chip and entire system on which it is based, insecure.

Shields to protect a chip from the above attacks exist at present; they are typically divided into two categories, active and passive. Passive shields are simple metal layers over all or part of the circuit and are designed to prevent viewing and probing. Passive shields may be removed by chemical, plasma or other techniques without changing the operation of the circuit. In other words, a passive shield works to deter attackers by making viewing more difficult initially, but will not actively defend itself against removal.

Active shields may look similar or may look more like a network of lines covering all or part of a circuit. If a line or part of the shield is removed,

severed or short-circuited to another line, the breach is detected and the chip halts some or all functions.

Active shields may still be breached using, for example, the following technique. An active shield line is identified as above the circuit element to be attacked. This shield line is bypassed using the ability of the FIB system previously mentioned. The bypass is in the form of a diversion track added in parallel to the original shield track. The original shield track may now be removed leaving the new bypass to fool the detection circuit. No circuit break is detected.

SUMMARY OF THE INVENTION

The present invention, in preferred embodiments thereof, comprises an active shield made in such a way that individual tracks are not visible by any normal microscopy technique. The tracks are preferably present in a layer of semiconductor material. The tracks preferably comprise doped regions separated by semi-insulating regions of either undoped material, or differently doped material. The tracks are doped sufficiently to allow conduction of electronic carriers. Between the tracks, the material, doped or undoped, is depleted of carriers. This region is rendered semi-insulating through the lack of intrinsic or extrinsic carriers, or through the trapping of such carriers. The conductive region is formed into tracks which form part of an active shield as described above. Most preferably, the conductive lines and the insulating regions between them are made in the same way and look identical to all analytical techniques. An attacker therefore does not know where to bypass the active shield lines.

BRIEF DESCRIPTION OF THE DRAWINGS

The present invention will be understood and appreciated more fully from the following detailed description, taken in conjunction with the drawings in which:

Fig. 1 is a simplified pictorial illustration of an integrated circuit protected by chip shielding, constructed and operative in accordance with a preferred embodiment of the present invention; and

Fig. 2 is a simplified pictorial illustration of a top view of the integrated circuit of Fig. 1.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

The present invention, in preferred embodiments thereof, provides a method to protect a security chip from invasive attacks. Preferably, a layer is added above the layers of the circuit to be protected from attack. The added layer may be made of polycrystalline silicon, as this material is commonly used in the manufacturing cycle of integrated circuits, but may alternatively be made of many other suitable materials. Any material whose conductivity can be materially changed without being visibly different would be a candidate for the material to be used in the added layer. The added layer is typically applied towards the end of the chip manufacturing process, and is applied above the normal circuit interconnect layers. The added layer may also be protected by a passivation layer, as is typically used in such integrated circuits.

The added layer is preferably implanted with dopants to allow conduction. In one preferred embodiment of the present invention dopants are selectively implanted in tracks corresponding to where the designer wants them placed. Dopants may be implanted in the material by high energy ion bombardment or by any other appropriate method.

In another preferred embodiment of the present invention utilizes either blanket bombardment of the layer with dopant ions or incorporation of the dopants during the growth of the layer. This latter approach will typically be achieved in the case of doped polysilicon, by CVD growth using silane gas for silicon growth and boron trichloride gas for dopant species.

However the growth and dopant incorporation is achieved, it must be done in such a way that the incorporated dopant atoms are not active. This means that the dopant atoms are not on designated sites as substitutes for the main material atoms. This means that the dopant atoms are interstitial, or between their normal, substitutional sites. This further means that the dopant atoms do not contribute carriers to conduction processes in the layer. This means that the material, as grown, is semi-insulating and does not conduct.

A further step in the creation of the shield layer is the selective activation of the dopants described above. The selective activation is typically achieved through an annealing process. This annealing process is effective if the

material is heated to a temperature close to (typically, within approximately 100 degrees C of) its melting point. In one preferred embodiment, the doped polysilicon is rapidly brought up to the annealing temperature by irradiation from a pulsed light source. The pulsed light source may be an infrared laser. The laser may be a YAG laser (Yttrium Aluminium Garnet, output wavelength 1064 nm). This laser may be driven in pulsed mode with a q-switch to limit the on-time to several nanoseconds or faster. The high power density during the pulse must be sufficient to anneal the dopants in that region of the material. In addition, the power density during the pulse must not be sufficient to ablate the material or cause damage to active circuit layers.

Conductive tracks are patterned into the layer by the annealing action. The laser, for example, may be scanned across the surface. The pattern of scanning is immaterial but may be raster scanning or following the semi-random path of a tracks path from start to end, or most efficiently, by alternate direction scanning (boustrephorous scanning) of the surface. The annealing will locally activate the dopants in the tracks required.

The annealing must be such that the conductive tracks are physically similar in all important respects to the semi-insulating material between the tracks. An attacker cannot "see", by normal analytical means, the tracks to be bypassed in an attack.

Reference is now made to Fig. 1, which is a simplified pictorial illustration of an integrated circuit protected by chip shielding, constructed and operative in accordance with a preferred embodiment of the present invention. This figure shows the basic construction of an integrated circuit with a silicon (single crystal) substrate on top of which are constructed gates and other active and passive circuit elements interconnected by networks of (typically) aluminium tracks. As these aluminium tracks are vulnerable to attack a layer of polysilicon is shown above them to illustrate the position of the protective shield layer.

Reference is now made to Fig. 2, which is a simplified pictorial illustration of a top view of the integrated circuit of Fig. 1. This figure shows a top down view of the protective shield layer. The serpentine track illustrates one method, as described above, of writing a serpentine conductive line in this

material. As described above, this can be achieved by scanning a pulsed infra-red laser over the areas to be annealed. The annealing activates the dopants in this region, allowing conduction along the track. The track may be connected to the underlying circuitry using, for example, tungsten plugs as vias.

It is appreciated that various features of the invention which are, for clarity, described in the contexts of separate embodiments may also be provided in combination in a single embodiment. Conversely, various features of the invention which are, for brevity, described in the context of a single embodiment may also be provided separately or in any suitable subcombination.

It will be appreciated by persons skilled in the art that the present invention is not limited by what has been particularly shown and described hereinabove. Rather the scope of the invention is defined only by the claims which follow:

What is claimed is:

CLAIMS

1. Apparatus substantially as described hereinabove.

2. Apparatus substantially as shown in the drawings.

3. A method substantially as described hereinabove.

4. A method substantially as shown in the drawings.

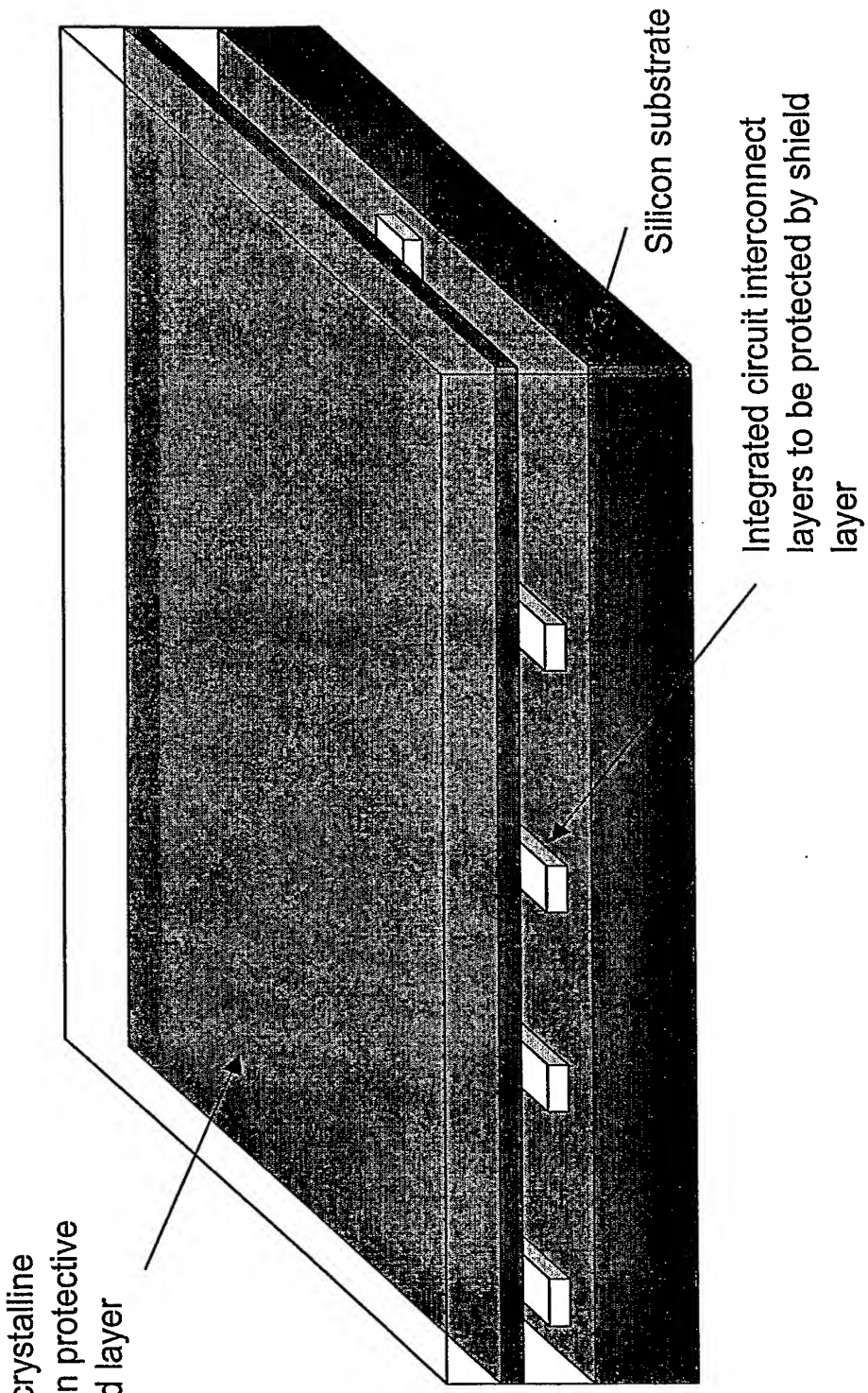

Polycrystalline
silicon protective
shield layer
Silicon substrate
Integrated circuit interconnect
layers to be protected by shield
layer

Fig. 1

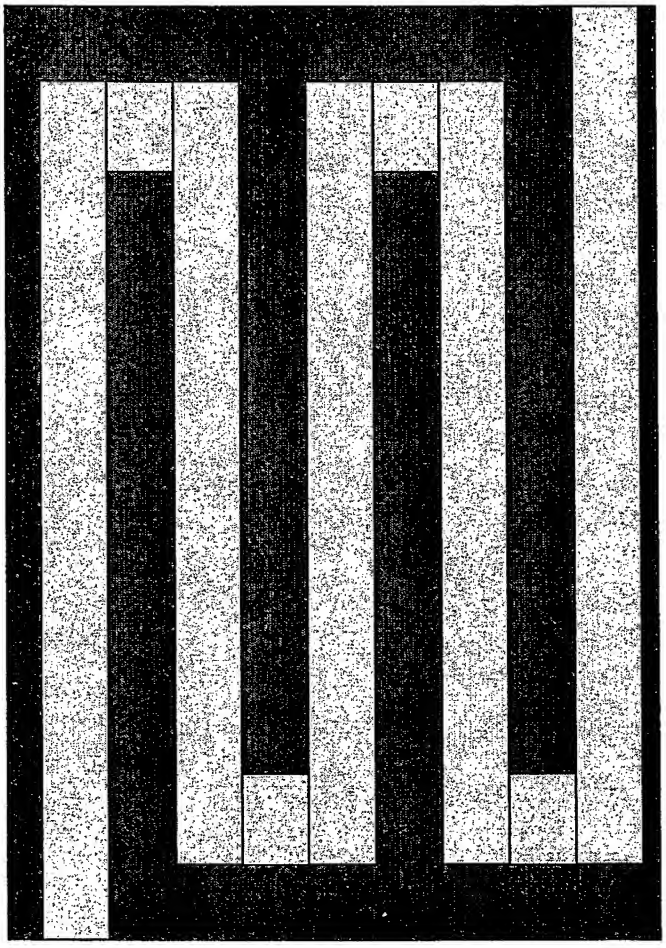


Fig. 2